UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,677	03/03/2004	Mohammad K. Ibrahim	3055/12	2304

22429 7590 09/21/2007
LOWE HAUPTMAN HAM & BERNER, LLP
1700 DIAGONAL ROAD
SUITE 300
ALEXANDRIA, VA 22314

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/790,677	IBRAHIM, MOHAMMAD K.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 9-13, 17-22* is/are rejected.

7)☒ Claim(s) *6-8 and 14-16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/3/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-22 have been examined.

Claim Objections

2. Claims 1, 2, 9, 17 and 18 are objected to because of the following informalities:

Claims 1 recites the limitation "the addition of points". There is insufficient antecedent basis for this limitation in the claim.

Claims 1 and 9 recite the limitation "the receiving correspondent". There is insufficient antecedent basis for this limitation in the claim.

Claims 1 and 9 recites the limitation "the corresponding mathematical". There is insufficient antecedent basis for this limitation in the claim.

Claim 17, recites the limitation "the improvement". There is insufficient antecedent basis for this limitation in the claim.

Claim 17, recites the limitation "the Z-coordinate". There is insufficient antecedent basis for this limitation in the claim.

Claim 18, recites the limitation "the addition". There is insufficient antecedent basis for this limitation in the claim.

Claim 2 doesn't end with a period.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-5, 9-13 and 17-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Kurumatani US 6,876,745 B1.

5. As per claims 1 and 9, Kurumatani teaches a method for communicating securely over an insecure communication channel between a pair of correspondents who perform shared key cryptographic operations by implementing respective ones of a pair of complimentary mathematical operations utilizing a shared key, said method comprising the steps of:

assembling a data string including information to be transferred from a sending correspondent to a receiving correspondent [column 8, lines 41-52 and column 9, lines 7-22];

performing a complimentary mathematical operation using points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the addition of points on the elliptic curve is defined in projective coordinates [column 11, lines 1-33 and column 12, lines 40-65]; and

forwarding the defined group of points over a communication channel to the receiving correspondent and performing the other of the corresponding mathematical cryptographic operations to decrypt the data [column 8, lines 41-52, column 9, lines 7-22 and figures 1 and 10].

6. As per claim 17, Kurumantani teaches, In a method for communicating securely over an insecure communication channel using elliptic curve cryptography an improvement comprising applying projective coordinated in two stages and wherein a projective coordinate in a first of

said stages is used to embed extra message data bits in the Z-coordinate and wherein a projection coordinate in a second of said two stages is used to improve a division operation at each iteration and for randomizing the computation in order to provide a counter measure against differential power analysis (i.e., multiplying individual projective coordinates by a random number K, column 11, lines 1-33 and column 12, liens 40-65).

7. As per claim 18, Kurumantani teaches a method of digital signatures generation and verification using points on an elliptic curve defined over a finite field and represented in projective coordinates, and wherein the addition of points on the elliptic curve is defined in projective coordinates [column 8, lines 47-64 and column 11, lines 1-5].

8. As per claims 2 and 10, Kurumantani further teaches the method where the elliptic curve points in projective coordinates are represented using three coordinates, (X,Y,Z), wherein X, Y and Z are elements of F(p) represented in N-bit strings, and which includes a step where extra message bits are embedded in the Z coordinate in addition to the message data bits that are embedded in the X coordinate [column 11, lines 1-33].

9. As per claims 3-5 and 11-13, Kurumantani further teaches the method comprising the steps of: embedding a message bit string into the X and Z coordinates of an elliptic curve point which is designated as the message point, (X.sub.mY.sub.m,Z.sub.m), providing a shared key k and a base point (X.sub.bY.sub.bZ.sub.b) and computing the scalar multiplication (X.sub.bkY.sub.bkZ.sub.bk)=k (X.sub.bY.sub.bZ.sub.b), computing a cipher point (X.sub.cY.sub.cZ.sub.c) using (X.sub.cY.sub.cZ.sub.c)=(X.sub.mY.sub

.mZ.sub.m)+k(X.sub.bY.sub.bZ.sub.b), sending appropriate bits of the X-coordinate, X.sub.c and the Z-coordinate Z.sub.c of the cipher point (X.sub.cY.sub.cZ.sub.c) to a receiving party; using the shared key k and the base point (X.sub.bY.sub.bZ.sub.b) computing the scalar multiplication (X.sub.bkY.sub.bkZ.sub.bk)=k (X.sub.bY.sub.bZ.sub.b), computing the message point (X.sub.mY.sub.mZ.sub.m) using (X.sub.mY.sub.mZ.sub.m)= (X.sub.cY.sub.cZ.sub.c)+(-k (X.sub.bY.sub.bZ.sub.b)), recovering the message bit string from X.sub.m and Z.sub.m [column 11, lines 1-33 and column 12, lines 40-65].

10. As per claim 19, Kurumantani further teaches the method which involves mathematical operations that includes steps of elliptic curve scalar multiplication(s) using point additions defined in projective coordinates [column 11, lines 1-33 and column 12, lines 40-65].

11. As per claim 20, Kurumantani further teaches the method where both the X and Z coordinate of the computed elliptic curve point(s) are used in the signature generation and verification steps [column 11, lines 1-33, column 12, lines 40-65 and figure 10].

12. As per claims 21 and 22, Kurumantani further teaches the method in which a second projective coordinate is used by the signing correspondent and to the verifying correspondent to eliminate the inversion or division during each addition and doubling operation of the corresponding scalar multiplication, and for randomizing the computation in order to provide a counter measure against differential power analysis [abstract and column 11, lines 1-33].

Allowable Subject Matter

13. Claims 6-8 and 14-16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

September 13, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100